Deciding whether a quantum state has secret correlations is an NP-complete problem

Jae-Weon Lee,[*] DoYong Kwon,[†] and Jaewan Kim[‡]
School of Computational Sciences, Korea Institute for Advanced Study, Seoul 130-722, Korea

(Dated: February 1, 2008)

From the NP-hardness of the quantum separability problem and the relation between bipartite entanglement and the secret key correlations, it is shown that the problem deciding whether a given quantum state has secret correlations in it or not is in NP-complete.

PACS numbers: 03.65.Ud , 03.67.Lx, 89.20.Ff

Recent progress in theories and experiments on quantum key distribution (QKD) allows one to think QKD as the first successful application of quantum information science[1]. However, minimal and essential physical ingredients for QKD are still not clear. For example, the equivalence between bipartite entanglement and secret key generation is still unproved[2]. Acin et al. [3] showed that, under the assumption that legitimate parties measure only single copies of the state and eavesdropper performs individual attack, secret bits can be asymptotically distilled from any two-qubit entangled state. Recently, in Ref. [4, 5] it was shown that entangled states can be mapped into classical probability distributions containing secret correlations and vice versa. It was also shown that, surprisingly, even from bound entangled states one can distill an arbitrarily secure key [6]. All these results give rise to a fundamental question about exact connections between entanglement of a quantum state and the private key distillable from the state [7]. On the other hand, in computational science there is a long standing open problem called P vs. NP problem; *Is an easy checkable problem always easy solvable*[8]? Many practical classical cryptography systems such as RSA[9] and Elliptic curve cryptography[10, 11] rely on difficulty of some mathematical problems in NP class for security, while security for quantum key distribution (QKD) systems relies on physical laws. In this paper a relation between this famous computational complexity problem and quantum key distribution is investigated. More precisely, we show that deciding whether a given quantum state has secret correlations (*i.e.*, $I_{form}(X;Y|Z) > 0$, see below) in it or not is in NP-complete class.

Let us begin by shortly reviewing the secret key generation from a given *classical* distribution $P(X,Y,Z)$ of random variables X, Y, and Z. This distribution might have been obtained from measurements of shared states independently done by legitimate parties, Alice(M_X) and Bob(M_Y), and an eavesdropper Eve(M_Z). Then, for a given $P(X,Y,Z)$ a secret key rate $S(X;Y||Z)$ is the maximum key generation rate from the distribution by local operations and public classical communication(LOPC). Similarly, one can define the information of formation $I_{form}(X;Y|Z)$ which is the amount of secret bits needed for preparing $P(X,Y,Z)$. They satisfy a relation[12]

$$S(X;Y||Z) \leq I(X;Y|Z)_{form}, \tag{1}$$

which states that as the entanglement cost is larger than or equal to distillable entanglement, so the amount of secret bits needed for preparing the distribution is larger than or equal to the amount of secret bits that is distillable from it. There is a well known following theorem on the relation between bipartite entanglement of a state and the secret correlations in it.

Theorem 1 (Equivalence of bipartite entanglement and secret correlation). *[4, 5] Let $|\psi_{ABE}\rangle$ be a pure quantum state shared by Alice, Bob, and Eve, such that the state is a purification of Alice and Bob's bipartite density matrix ρ_{AB} (*i.e.*, $\rho_{AB} = tr_E(|\psi_{ABE}\rangle\langle\psi_{ABE}|)$. Then, ρ_{AB} is entangled if and only if there exist measurements of $|\psi_{ABE}\rangle$ by Alice (M_X) and Bob (M_Y), such that for any measurement by Eve (M_Z), the corresponding probability distribution $P(X,Y,Z)$ contains secret correlations,*i.e., $I_{form}(X;Y|Z) > 0$.

This theorem is proven by showing the existence of an entanglement witness from the measurement operators M_X and M_Y. In this paper we will consider only bipartite states in $\mathcal{H}_A \otimes \mathcal{H}_B$ where $dim(\mathcal{H}_A) = M$ and $dim(\mathcal{H}_B) = N$.

Since Turing machines can not represent arbitrary real or complex numbers from now on we deal with only density matrices of which representations $[\rho]$ have rational entries with finite precision. Now we define a problem deciding whether a given state has secret correlations.

Definition 1 (Quantum Secret Correlation problem(QSCORR)). *Let $[\rho_{AB}]$ be a rational bipartite mixed state having a purification $|\psi_{ABE}\rangle$ as described in Theorem 1. Given $[\rho_{AB}]$, does any $P(X,Y,Z)$ from $|\psi_{ABE}\rangle$ contain secret correlations, that is, $I_{form}(X;Y|Z) > 0$?*

To tackle this problem we need the famous theorem by Gurvits[13, 14] about deciding entanglement of a given density matrix on a (deterministic) Turing machine (*i.e.*, an abstraction of ordinary computers). To understand the theorem let us recall some definitions in computational complexity theory[8]. We say that a problem A is polynomially reducible to another problem B if there

[*] Electronic address: scikid@kias.re.kr
[†] Electronic address: doyong@kias.re.kr
[‡] Electronic address: jaewan@kias.re.kr

exists a polynomial-time algorithm that converts each input(instance) I_A of A to another input I_B of B such that I_A is a *yes*-instance of A if and only if I_B is a *yes*-instance of B. In this case we denote this relation as $A \leq_P B$. The NP (Non-deterministic Polynomial time) class is the set of decision problems that can be verified by a Turing machine in polynomial time. Many practical and important problems such as the factoring (a decision version) and the graph isomorphism problem belong to this class. The NP-hard class is the class of all problems B such that for every problem in NP there exists a polynomial time reduction to B. Many interesting physical problems belong to this class[15]. The NP-complete class is an intersection of the NP class and the NP-hard class.

One can naturally imagine the following separability problem of rational density matrices.

Definition 2 (Rational quantum separability problem (EXACT QSEP))**.** *Given a bipartite rational $[\rho]$, is $[\rho]$ separable?*

Unfortunately, EXACT QSEP encounters a mathematical difficulty near the boundary of $S_{M,N}$[16, 17] about representing density matrices with rational numbers. Here $S_{M,N}$ is a convex set of separable density matrices acting on $\mathcal{H}_A \otimes \mathcal{H}_B$. Instead, Gurvits considered a problem asking whether a given $[\rho]$ is close to separable states[13].

Definition 3 (Weak membership problem (WMEM))**.** *Given a rational vector $[\rho]$ and a rational $\delta > 0$, assert that either*

$$[\rho] \in S(S_{M,N}, \delta), \text{ or} \tag{2}$$

$$[\rho] \notin S(S_{M,N}, -\delta), \tag{3}$$

where $S(S_{M,N}, \delta)$ is a union of all δ-balls of which centers belong to $S_{M,N}$ and $S(S_{M,N}, -\delta)$ is a set of centers of δ-balls where the δ-balls are contained in $S_{M,N}$.

Deciding, quantifying and distillating entanglement are subjects of intensive investigations in quantum information community[18]. For example, an improved algorithm for quantum separability and entanglement detection on classical computers is suggested[19] and Doherty *et al.* constructed families of operational criteria for separability based on semidefinite programs[20]. Despite all these efforts an efficient (*i.e.*, polynomial time) algorithm for the separability problem is still unknown. The following seminal theorem due to Gurvits explains why the quantum separability problem is so hard.

Theorem 2 (Gurvits)**.** *WMEM for $S_{M,N}$ is NP-hard with respect to the complexity-measure $(N + <[\rho]> + <\delta>)$ if $N \leq M \leq \frac{N(N-1)}{2} + 2$, where $<>$ denotes the size of the encoding.*

He demonstrated a polynomial time reduction from an NP-complete problem called KNAPSACK to WMEM($S_{M,N}$) after a series of transformations.

At first glance, it might seem that knowing Theorem 1 and Theorem 2 one can easily prove the NP-completeness of the problem deciding whether a given state has secret correlations(QSCORR). But real situation is complicated. To be proved as an NP-complete problem, the problem should be a decision problem. However, WMEM is not a decision problem, because inputs corresponding to states near the boundary of $S_{M,N}$ can give both possible answers[16]. To avoid this ambiguity Ioannou designed a decidable separability problem called QSEP[16] asking whether, given a rational density operator $[\rho]$, there exists a separable density operator σ close to $[\rho]$.

Definition 4 (QSEP)**.** *Given a rational bipartite density matrix $[\rho]$ acting on $\mathcal{H}_A \otimes \mathcal{H}_B$, and p-bit rational numbers ϵ and δ'; does there exist a separable state $\sigma = \sum_{i=1}^{M^2N^2} p_i|\alpha_i\rangle\langle\alpha_i| \otimes |\beta_i\rangle\langle\beta_i|$, of which p-bit truncated and unnormalized version $\tilde{\sigma} = \sum_{i=1}^{M^2N^2} \tilde{p}_i|\tilde{\alpha}_i\rangle\langle\tilde{\alpha}_i| \otimes |\tilde{\beta}_i\rangle\langle\tilde{\beta}_i|$ satisfying*
i) $|[\rho] - \sigma|_2 < \delta'$, and
ii) $|\sigma - \tilde{\sigma}|_2 < \epsilon$?
Here $|A-B|_2 \equiv \sqrt{tr((A-B)^2)}$, $\tilde{p}_i \geq 0$ is a p-bit rational number and $p_i \geq 0$.

We have adopted a slightly modified definition from the original one of QSEP in [16] for our purpose, but basically two definitions are equivalent.

Theorem 3. *QSEP is in NP-complete[16].*

The NP-completeness of QSEP was proven by reduction from WMEM. QSEP is carefully designed so that for an instance $I([\rho], \delta)$ of WMEM one call QSEP with an instance $I'([\rho], p, \epsilon, \delta')$ such that $\delta \geq \delta' + \epsilon$. To utilize this definition we consider a negation of QSCORR with error.

Definition 5 (No Quantum Secret Correlation (NQSCORR))**.** *Given a rational bipartite density matrix $[\rho]$, does there exist a state σ, satisfying*
i) $|[\rho] - \sigma|_2 < \delta'$,
ii) $|\sigma - \tilde{\sigma}|_2 < \epsilon$, and
iii) for any purification $|\psi_{ABE}\rangle$ of σ as described in Theorem 1, it contains no secret correlations, that is, $I_{form}(X;Y|Z) = 0$? (Here δ',ϵ are p-bit rational numbers and $\tilde{\sigma}$ is a p-bit truncation of σ)

Note that in the zero-error limit ($\delta' \to 0, \epsilon \to 0$) this problem reduces to the exact negation of *QSCORR*.

Theorem 4. *NQSCORR is in NP-complete.*

Proof. Basically, this theorem is a corollary of Theorem 1 and Theorem 3. If there is an algorithm that solves NQSCORR, then one can call the algorithm to solve QSEP. More precisely, given $I([\rho], p, \delta', \epsilon)$ of QSEP one can call NQSCORR with $I'([\rho], p, \delta', \epsilon)$. NQSCORR returns *yes* if and only if QSEP returns *yes* because of the equivalence of bipartite entanglement and secret correlations (Theorem 1). This means NQSCORR is at least as hard as QSEP which is in NP-complete class. Therefore NQSCORR is also in NP-hard. Furthermore, given a certificate $(\tilde{\sigma}, M_X, M_Y, M_Z)$ one can quickly (*i.e.*, in a polynomial time) verify whether $I_{form}(X, Y|Z)$ from $P(X, Y, Z)$ is positive or not. Hence NQSCORR is also in NP. Therefore, NQSCORR is in NP-complete class. □

The full reduction chain is $KNAPSACK \leq_P RSDF \leq_P WVAL \leq_P WMEM \leq_P QSEP \leq_P NQSCORR$ (See [13, 16] for definitions of the intermediate problems).

One may think of another related and more interesting problem asking whether a given bipartite density matrix has non-zero secret key generation rate, that is, $S(X, Y||Z) > 0$. Since $I_{form}(X; Y|Z) > 0$ is not a sufficient condition but a necessary condition for $S(X, Y||Z) > 0$, (*i.e.*, there is a bound information[21]), we could not answer to this interesting question within our approach.

What our results imply is that there is no easy procedure or simple formula for deciding whether a given quantum state gives rise to secret correlations if $P \neq NP$ (which is usually believed). Conversely, as a byproduct of our results, if one can find a polynomial time algorithm solving the NQSCORR problem on a deterministic Turing machine it means $P = NP$. Our results also reveal that the P vs. NP problem is not only related to classical cryptography but also to quantum cryptography in a different way.

Acknowledgments

We thank Joonwoo Bae and Sung-il Pae for helpful discussions. J. Lee and J. Kim was supported by the Korea Ministry of Information and Communication with the“Next Generation Security Project”.

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[2] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, quant-ph/0506189 (2006).

[3] A. Acin, L. Masanes, and N. Gisin, Phys. Rev. Lett. **91**, 167901 (2003).

[4] A. Acin and N. Gisin, Phys. Rev. Lett. **94**, 020501 (2005).

[5] M. Curty, M. Lewenstein, and N. Lütkenhaus, Phys. Rev. Lett. **92**, 217903 (2004).

[6] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, Phys. Rev. Lett. **94**, 160502 (2005).

[7] R. Augusiak and P. Horodecki, Phys. Rev. A **74**, 010305 (2006).

[8] C. Papadimitriou, *Computational Complexity* (Addison-Wesley, Newyork, 1994).

[9] R. Rivest, A. Shamir, and L. Adleman, Communications of the ACM **21**, 120 (1978).

[10] N. Koblitz, Mathematics of Computation **48**, 203 (1987).

[11] V. Miller, CRYPTO 85 (1985).

[12] U. Maurer and S. Wolf, IEEE Trans. Inf. Theory **45**, 499 (1999).

[13] L. Gurvits, Proceedings of the 35th ACM Symposium on Theory of Computing ACM Press, New York, 2003 p. 10 (2003), quant-ph/0303055.

[14] L. Gurvits, J. Comput. Syst. Sci. **69**, 448 (2004).

[15] J. Eisert, quant-ph/0609051 (2006).

[16] L. M. Ioannou, quant-ph/0603199 (2006).

[17] O. Guhne and N. Lütkenhaus, Phys. Rev. Lett. **96**, 170502 (2006).

[18] D. Bruss, Journ. Math. Phys. **43**, 4237 (2002).

[19] L. M. Ioannou, B. C. Travaglione, D. Cheung, and A. K. Ekert, Phys. Rev. A **70**, 060303 (2004).

[20] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri, Phys. Rev. Lett. **88**, 187904 (2002).

[21] A. Acin, J. I. Cirac, and L. Masanes, Phys. Rev. Lett. **92**, 107903 (2004).